Formación en Inteligencia Artificial

Hernando Bermúdez Gómez

Una de las consecuencias de la estrategia comercial que nos rodea es que muchos se sienten capaces de usar y aprovechar herramientas de inteligencia artificial, aunque esto sea una gran mentira. Sencillamente los ignorantes son capaces de depositar confianza en todo lo que se les diga, porque carecen del juicio y el conocimiento para evaluar las respuestas de las aplicaciones en comento. Revisando ISACA (the Information Systems Audit and Control Association, Inc.,) encontramos que hace tiempo viene trabajando para formar expertos en el tema. Así nos encontramos con tres programas: AI Risk Governance and Framework Integration, AI Life Cycle Risk Management y AI Risk Program Management. Ahora se está anunciando la Advanced in AI Risk (AAIR) certification. ISACA precisa: "*The credential is designed to refine and strengthen existing risk management expertise, empowering IT risk professionals to tackle the evolving challenges and opportunities that come with AI integration. —To qualify, candidates must have proven experience in IT risk or advisory roles, as well as hold one of 25 prerequisite certifications, such as CISA, CISM, CRISC, CGEIT, CDPSE, CRMP, CRMA, CGRC, CISSP, CERP, or CRCM, in addition to passing the certification exam. —Additional resources are available to those seeking to become AAIR certified, including the AAIR Online Review Course, the AAIR Questions, Answers & Explanations Database, and the AAIR Review Manual (available as a digital or print version).*" Así debe ser. No cualquiera puede presentarse como experto, ni ha de ser admitido a estudios avanzados. Además de cursar y aprobar las materias incluidas en el programa los estudiantes deben demostrar, mediante pruebas, que son capaces de: 1. Evaluate risk related to AI models/solutions including design, suitability, algorithms, training, drift, and AI life cycle. 2. Facilitate the integration of AI risk management into an enterprise risk management framework and risk programs. 3. Develop and implement an AI risk management framework, including roles and accountability, AI risk policies and procedures, and acceptable risk tolerance levels. 4. Conduct risk assessments to identify and classify risks associated with AI. 5. Develop and recommend risk treatment strategies for identified AI risks. 6. Assess compliance with applicable AI-related regulations, laws, frameworks, standards, and guidelines. 7. Integrate AI risk considerations into existing governance programs. 8. Integrate AI risk considerations into existing risk register and control taxonomies. 9. Evaluate AI use cases based on the organization's risk appetite. 10. Monitor and test organizational processes to identify AI risks. 11. Collaborate with stakeholders to develop and integrate AI risk concepts into enterprise-wide awareness training. 12. Capture AI risk considerations in enterprise risk metrics and reporting (e.g., board, management, operations). 13. Conduct and/or evaluate threat and vulnerability assessments on AI projects/programs. 14. Collaborate with stakeholders to integrate AI risk scenarios into the enterprise incident management program. 15. Continuously assess and

monitor the risk landscape for emerging AI risk. 16. Evaluate controls to manage AI-related risk within the organization's risk tolerance. 17. Advise on AI-related risk within contracts and service agreements, including data usage and intellectual property. 18. Evaluate AI risk as part of supply chain risk management. 19. Collaborate with stakeholders to address AI trustworthiness and impacts including ethics, bias, privacy, safety, and environmental, social, and governance (ESG) implications. 20. Leverage AI to support the risk management program (e.g., risk profile, reporting, evaluation, risk models, and analysis). 21. Integrate AI-related risk considerations into the change management process. 22. Incorporate AI-related risk considerations into incident response, BIAs, the BCP, and DRP. 23. Assess human oversight controls at critical decision points for risk and AI impact.

Algunos contradores piensan que ellos son muy competentes en tecnología pero eso está por verse desde la perspectiva de los correspondientes ingenieros.

Bogotá, abril 22 de 2026.